AI Secured SD-WAN Architecture as a Latency Critical IoT Enabler for 5G and Beyond Communications

Rameez Asif and Kinan Ghanem
Department of Electronics and Electrical Engineering, University of Strathclyde, Glasgow, UK
Power Networks Demonstration Centre (PNDC), University of Strathclyde, Glasgow, UK
Corresponding Author: rameez.asif@strath.ac.uk

***Abstract*— Software-defined Wide Area Network (SD-WAN) is an elementary change in the way network architects and service providers transpose their focus from hardware to the software oriented paradigm. Using a virtual network overlay, SD-WAN classifies and prioritizes how each application goes through the network based on business priority, quality of service (QoS), service-level agreements (SLAs) and security requirements. In this paper, we presented a system level concept and implementation of AI secured SD-WAN technology that is helping service providers to easily connect to and integrate across all the different IoT compute edges required to optimize the traffic and management of 5G cells. This architecture will enable a seamless transition for energy sector towards a full 5G connectivity by managing any data available across the edge, leveraging 5G transport for those critical applications that require ultra-low latency and higher bandwidths. Moreover, we weigh the pros and cons of using hybrid Multi-protocol Label Switching (MPLS) with SD-WAN to provide seamless integration, scalability and flexibility to the energy sector.**

I. INTRODUCTION

Virtualization is an enabling network architecture to design, implement, and manage network services far more efficiently than ever before [1]. Software-defined networking (SDN) and network functions virtualization (NFV) are two of the key capabilities fostering this transformation. SDN manages networks by separating the control plane from the forwarding plane. Network architects and enterprises use software to configure and manage network functions via a centralized control server [2]. This approach creates dynamic, agile, secure and scalable networks that use the virtualized infrastructure of modern data centers to respond rapidly to changing business requirements. Whereas, NFV decouples functions from proprietary hardware appliances (routers, firewalls, VPN terminators, SD-WAN, etc.) and delivers equivalent network functionality without the need for specialized hardware [3]. These virtual network functions (VNF) run on high-performance computing machines and offer the distinct advantage of on-demand deployment.

Virtual network functions deployed in the dense IoT networks via mobile edge computing (MEC) are enabling enterprises to take advantage of SDN capabilities to modernize communication networks deliver new services, establishing new connections, and optimizing the performance [4]. With the help of SDN, the virtual routers deployed at the data centers eliminate backhaul delays by establishing secure, ultra-low latency connections between applications and data hosted in multiple clouds. Moreover, intelligent virtual firewalls protect the communication networks from external cyber attacks originating from the applications hosted on public clouds [5].

Legacy Wide-Area-Networks (WAN) architectures, like MPLS-IP and MPLS-TP [6], create limitations as energy utilities adopt the cloud or utilize commodity Internet connections in their operational technology (OT) networks. The enterprises or energy sector, that is the main application discussed in this article, are shifting to Software-Defined Wide Area Network (SD-WAN) to ensure seamless cloud migration, reduced capital expenditure (CAPEX), infrastructure automation, virtualisation and improved user collaboration [7]. To demystify, the latest networking technological trends in IoT, we are presenting the system level review of the SD-WAN that are making use of data processing to strengthen next-generation firewalls for added security and privacy. We also studied the pros and cons of hybrid SD-WAN networks to provide seamless integration, scalability and flexibility to the existing infrastructure. This network architecture will not only benefit future 5G edge processing but also ease the latency and bandwidth requirements of IoT.

II. SECURE SD-WAN ARCHITECTURE

A Software-defined Wide Area Network (SD-WAN) is a virtualized WAN architecture that allows enterprises to leverage any combination of flexible communication layers [8], including MPLS, 5G/4G/LTE and fiber broadband Internet services, to securely connect end-users to data oriented applications, as depicted in Fig. 1. SD-WAN incorporates a centralized control function to intelligently and securely direct data across the WAN. This increases application performance and delivers a high quality-of-service (QoS), resulting in increased business productivity, agility and reduced costs for IT [9]. An SD-WAN platform that enables automation will help the energy sector to easily connect and integrate across all the different compute edges required to optimize the data and management of IoT and 5G cells. This will enable a seamless transition towards a full 5G infrastructure by managing any transport available across the edge, leveraging 5G transport for those critical applications that require zero latency and higher speeds [10]. SD-WAN can provide simplified WAN management, dynamic path optimization, cloud application deployment, distributed cloud

This is a peer-reviewed, accepted author manuscript of the following article: Asif, R., & Ghanem, K. (2021). AI secured SD-WAN architecture as a latency critical IoT enabler for 5G and beyond communications. In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) IEEE. https://doi.org/10.1109/ccnc49032.2021.9369477

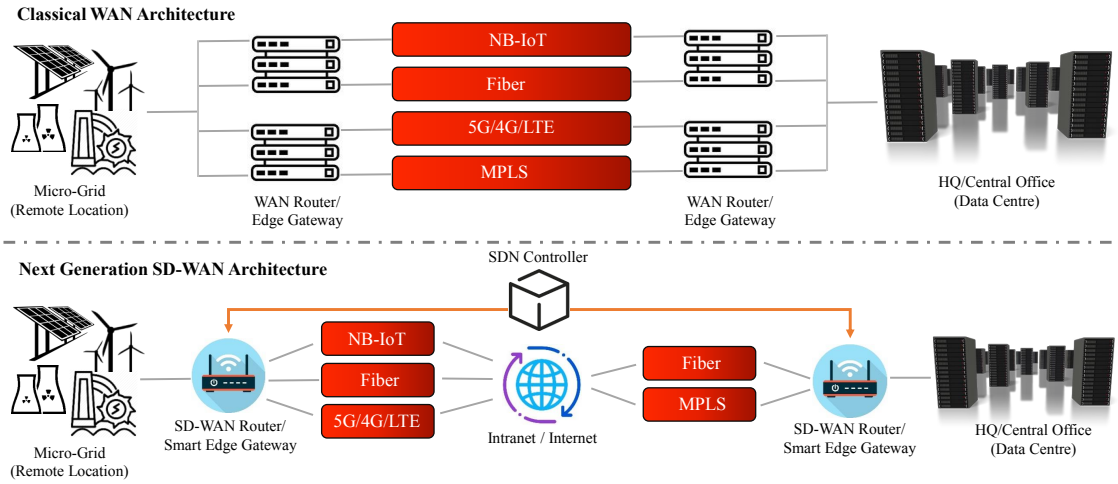

Fig. 1. Network architecture of classical WAN and next generation SD-WAN for energy utilities.

security and Network-as-a-Service (NaaS) [11].

The integration of cloud, next generation firewall (NGFW) and data analytics (artificial intelligence or machine learning) in SD-WAN can replace MPLS-IP or TP/MPLS, whose capabilities have been stretched to it‘s limit for bandwidth hungry applications and can no longer achieve the outcomes needed in today‘s world [12]. SD-WAN objective is to manage a single-pane, secure, streamlined connection for the most efficient path to applications and resources. So the enterprises can automate, centralize and simplify their network management functions. SD-WAN leverages the best of the cloud’s benefits:

- The ability to support multiple connection types (including MPLS, frame relay and 5G/4G/LTE wireless communications)
- Centrally-configured applications that provide a predictable user experience
- An intuitive interface that’s simple to configure and manage
- Less IT reliance on hardware
- Automatic provisioning that is easily and highly scalable (up to 10,000+ locations)

SD-WAN encompasses all elements of building and managing an overlay for various business needs, i.e. the centralized management, application policies, routing and interface support, analytics, and security [13]. And since it is integrated through the cloud, workflow and multi-cloud connectivity are all easily achieved, whether extending workloads to a private or public cloud or SaaS (Software-as-a-Service) [14]. With its distributed software, IP (Internet Protocol) capacity and standard hardware advantages, SD-WAN is a dependable, adaptable and cost-efficient alternative to MPLS.

The SD-WAN architecture, as in Fig, 1, has the ability to ensure resource allocation, automatic and dynamic path routing, which optimizes load balancing and resiliency. SD-WAN reduces network downtime, minimizing loss of productivity by detecting outages in real time which is beneficial for critical energy infrastructure [15]. In the event of an outage or fault on one of the communication path, automatic data path routing to available links keep your network running seamlessly. SD-WAN supports multiple secure high-performance connections, and allows for load-sharing across those connections. The scalability and flexibility to adjust data flows based on network conditions delivers the best quality-of-service under divers operating conditions [16].

III. AI Powered Next Generation Firewalls

Data driven next generation firewall (NGFW), integrated in SD-WAN enables us to foresee unknown threats, monitor data flow, IoT devices verification and authentication, and reduce errors with automatic policy recommendations [17]. While the legacy firewall typically provides collaborative inspection of incoming and outgoing network data, a NGFW includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence. A NGFW should have the following functionalities:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

Due to increased end-to-end encryption and the rise of affordable artificial intelligence (AI) and machine learning (ML) modules, the security of the energy sector needs to evolve to keep up with today‘s external cyber threats. While next generation firewalls (NGFW) still provide a critical component in a layered security solution, still they need to incorporate AI and ML algorithms to provide “one box to protect it all” turn-key solution [17]. NGFW added support for stateful packet inspection and many other features to provide extra security. With the research still at early stages, the prevalence of NGFW deployments led hackers to send traffic outbound over transmission control protocol (TCP)/443 wrapped in hypertext transfer protocol secure (HTTPS) headers as this type of data obscures their

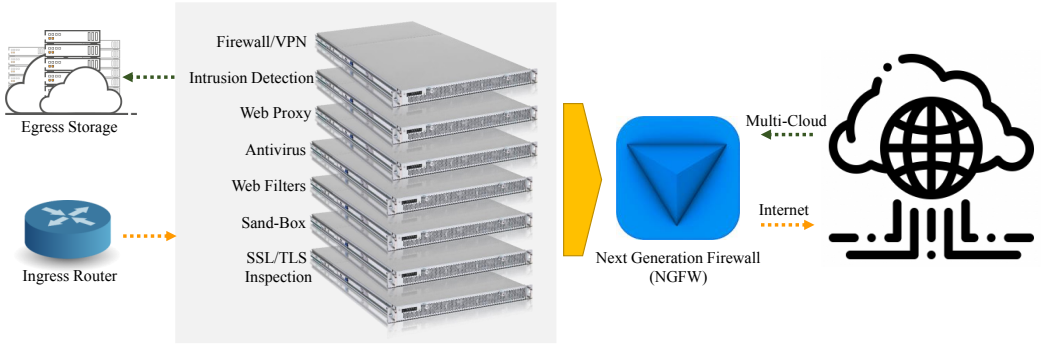

Fig. 2. Data driven next-generation firewall architecture for SD-WANs.

communications with the communications required for the end-user to access the Internet. Because HTTPS is end-to-end encrypted and necessary for enterprise productivity, nearly everyone allows it outbound from their network. In many cases, the hackers will send communications through a compromised domain to avoid triggering a DNS blacklist defeating another security layer (e.g. running their command and control software on a small business websites such as a e-commerce, health, pharmacies etc).

To protect the end-users and networks from the cyber attacks and malware, AI and ML are helping NGFW based on training on big data sets, as depicted in Fig. 2. Both data analysis methodologies has proven to be extremely useful when it comes to detecting cyber threats based on analyzing data and identifying a threat before it exploits a vulnerability in the deployed networks. Threats like Distributed Denial-of-Service (DDoS) attacks and Advanced Persistent Threats (APTs) exploiting telecommunication signaling protocols have shown that firewalls relying solely on rule-based firewalls (single protocol analysis) is not enough anymore [18]. Augmented rule-based firewalls are powered by AI enabling an immediate response to yet unknown external cybersecurity threats, which are undetectable by other legacy firewall and security solutions. By applying layered protection, as depicted in Fig. 3, that includes static and heuristic analysis, anomaly detection powered by machine learning, and sand-boxing, we provide operators a comprehensive defense with real-time, multi-layered threat detection. They can expedite the processes, by observing and learning network traffic patterns as well as suggesting security policies. Mainly, the enterprises have two main categories of polices in place.

- **Blacklist NGFW Policy** - allows all data to pass through the network unless it exhibits indicators that are known to be malicious and are included in the cyber policies. Blacklist NGFW lookup tables are easy to set-up and maintain, but are also fairly easy to bypass especially in the presence of AI and ML algorithms.
- **Whitelist NGFW Policy** - blocks all data by default unless it is specifically permitted by the cyber policies. For obvious reasons, whitelist NGFW lookup tables are more secure than blacklist WAFs, but are often much more difficult to set up and maintain. They also require a lot of ongoing tuning and maintenance, which is time consuming and prone to human error especially in the development of AI and ML algorithms for threat detection and data training.

IV. Hybrid MPLS / SD-WAN Architecture

Energy sector is deploying more service oriented applications in the cloud, bringing more devices the field that are consuming more bandwidth. Traditional connectivity options like MPLS can be costly as well as slow to provision, and offer limited bandwidth in many in dense networks. For this reason utilities are now adopting SDN based solutions for resource allocation and network provisioning. But moving to this new technology is difficult as legacy networks should have a seamless integration with newly deployed network. Most recently, hybrid MPLS and SD-WAN network architecture has been proposed to add flexibility, scalability and resilience in the classical WAN architecture [19]. By funneling traffic directly to the Internet, it eliminates extra hops and latency that can sometimes occur when traffic goes through a data center. This is one of the reason that SD-WAN is an ideal candidate for ultra-low latency applications in energy sector. Also, it is more cost effective because directing traffic over the Internet is less costly than using an MPLS link. Another benefit of a hybrid WAN, as depicted in Fig. 4, is that it allows the user to decide which communication framework is the best path back to data center by using real-time monitoring.

Enhancing the standalone infrastructures, as in Fig. 5, of energy utilities using MPLS technology can be very expensive. Any technology that promises to ease that expense

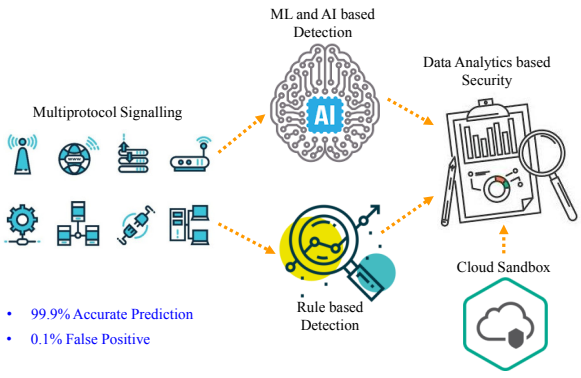

Fig. 3. AI and rule based next generation firewalls.

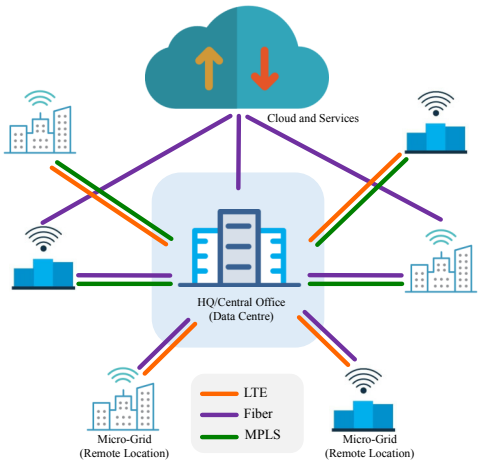

Fig. 4. Hybrid SD-WAN network architecture.

due to massive deployment of IoT edge devices, is worth considering. That is one of the main reason, SD-WAN is an important candidate for future extension plans. Several years ago, the security and privacy offered by MPLS was a point of discussion because hardware modules capable of encrypting data at high speeds were still very expensive. Moreover, encryption was not flexible in MPLS and multi-vendor device integration was not so easy [20]. Now, the general-purpose computing platforms present in most SD-WAN appliances are fast enough to encrypt data at high bandwidth that is acceptable for most situations, that allows the public Internet to be used for transport. SD-WAN can serve as a cost-savings method of replacing more expensive MPLS modules for diverse end-user applications in energy sector. However, like most technologies, it is not appropriate for all situations. Like the expensive appliances previously required to encrypt high volumes of data, this is still true with SD-WAN, since most appliances are using cost-effective processors, which have difficulty encrypting multiple gigabits per second of data. This particular constraint will also be alleviated over time as technology improves. Until then, private MPLS modules are still necessary when moving very high volumes of data over the WAN from hundreds of edge devices in the field.

Alongside privacy and encryption, Internet-based transport could not be considered a replacement for private connections because of the GDPR and policies to keep the consumer data for processing. Over time, this has also improved dramatically as enhancements to the underlying technologies have been developed, such as the advanced encryption techniques, Blockchain, network slicing etc. Despite the advancements in reliability, commodity Internet modules are still vulnerable to the external cyber attacks. SD-WAN attempts to overcome these limitations with signal processing techniques like Forward Error Correction (FEC) [21], but if your application requires this high level of performance, you may required to instal high performance edge devices that are power hungry. A service provider might not always strictly meet their service-level agreement (SLA) , but you will at least have a remediation process available to you. Since MPLS services remain private to a carrier (or a few carriers within inter-carrier agreements), you will usually have less latency across an MPLS modules than with a general Internet connection. SD-WAN promotes scalable and flexible Internet-only data, but it is highly recommended to use SD-WAN in combination with MPLS modules, when the energy sector needs performance and latency requirements associated with MPLS. The summarised characteristics of both the networks are enlisted in Tab. I. One of the major advantages of SD-WAN is that it is “transport-agnostic”, meaning the network can utilize any transport mode, regardless of who provides it or where the network edges are located.

V. SD-WAN and MPLS with Cloud Integration

Worldwide energy sector is transforming into much advanced digital, resilient and virtualized networks. Keeping in mind the long term demands of Digital Transformation (DX), energy utilities are turning networks more scalable, flexible and agile for seamless access to cloud. In the era of Mobile Edge Computing (MEC), resource allocation for data analytics on the nodes are very important [22]. Additional parameters to make a choice between SD-WAN and MPLS are the security threats, demands of the end-users, and evolving multi cloud ecosystem. All have set MPLS out of the consideration list for most digitally matured energy networks. The rapid developments in SDN and NFV being other reason which added credence to the MPLS downfall.

Over the last 2 years, SD-WAN is the biggest leap in the telecommunication industry. It not only promises greater operational agility but business resiliency and higher quality of user experience as well. Moreover, to lay the foundation of DX, Chief Information Officers (CIOs) first need to upgrade enterprise networking capabilities. Otherwise, embarking on new age technology and creating a data-driven environment is next to impossible. This section will explain the key benefits of adopting SD-WAN over MPLS in the energy sector.

- **Operational Bandwidth** - Meeting higher bandwidth and low latency demands using MPLS increases network deployment costs, wherein using SD-WAN, energy utilities leverage internet connection to gain higher bandwidth and high data-rates at lower cost.
- **Communication Frameworks** - MPLS allows either Internet Protocol (IP) based connectivity or Transport

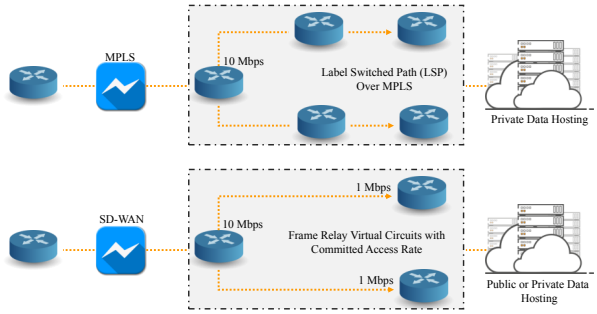

Fig. 5. Brief comparison of MPLS and SD-WAN network architectures w.r.t data rates and QoS.

TABLE I
SUMMARIZED DIFFERENCES BETWEEN MPLS AND SD-WAN NETWORK ARCHITECTURE.

	MPLS	SD-WAN (Including Hybrid Network)
Connectivity	Dual MPLS (Active Backup)	Combination of MPLS, 4G/LTE, Fiber connections
Cloud Access	Backhaul to data center and then to the cloud	Direct access to the cloud
Elasticity	Requires cost and time to extend the network	On the go expansion of the networks
Quality	Dedicated connections maintain good quality-of-service	Excellent maintenance of quality-of-service with flexible communication paths and policies
Security	Dedicated one-to-one link, but data has to be transmitted to data center for verification	Embedded security, AI powered firewalls, Auto VPN, segmentation, network silicing, cloud security

Profile (TP), whereas SD-WAN allows connections of all sort of legacy and next generation frameworks, e.g. MPLS, broadband, LTE, 4G, 5G etc. This flexibility makes SD-WAN a stronger candidate in multi-vendor devices environment for seamless integration.

- **Scalability and Performance** - Based on type of data and traffic priority different types of traffic are managed using Class of Service (CoS), SD-WAN leverage multiple ISP connections to send traffic along the best available path, ensuring higher performance.
- **Application Prioritization** - MPLS becomes inefficient when it comes comes to managing advanced data analytics, services and related applications. Using SD-WAN can leverage MPLS as well as broadband to route business critical applications and services selecting the best path available. These applications can be hosted in cloud or private data-centers where they can be deployed on the edge devices on-demand.
- **Cloud Integration** - Classical energy networks transmit the traffic to central data centres and where the data can be hosted in cloud. This can be expensive because utilities have to invest on the communication links with high bandwidth to transfer the raw data. Wherein SD-WAN connects directly to cloud making use of direct internet access (DIA) and since all the applications can he hosted on the edge devices, only selective useful data is transmitted to the cloud.
- **Security and Privacy** - The traffic transmitted to data centers is inspected using MPLS but security is often concentrated and traffic flows are configured and limited. Whereas, SD-WAN provisions auto VPNs, firewalls and advance network segmentation, slicing, encryption and Blockchain.
- **Network Visibility** - Using MPLS, additional management and monitoring tools is required to gain visibility of network and application performance. On the other hand, SD-WAN solution not only provide granular visibility to network intelligence but also allows networking teams to prioritize application according business intent.
- **Configurations and GUI** - Traditional WAN using MPLS required cumbersome manual configurations and upgradation. On the other hand SD-WAN has better graphical user interfaces (GUI) and connectivity that allows zero touch provisioning for applying any sort of changes or upgrades on the network.
- **Monitoring and Management** - Managing and monitoring traditional energy network infrastructure in distributed network ecosystems is challenging and time consuming. SD-WAN provides a centralized control to manage and monitor enterprise networks hassle free. Most of the advanced SD-WAN networks are supported by containerization (Docker) to provide virtualized monitoring and management. That translates into reduced down-time of the network.
- **Cost (CAPEX and OPEX)** - Reliance on standalone MPLS networks in energy sector means high cost, wherein SD-WAN allows the utilities to reduce cost by using cheaper internet links and alternative select-transmit options.

VI. USE-CASES FOR ENERGY UTILITIES

As the enterprises, especially energy sector, are rapidly adopting digital transformation the SD-WAN edge market has been evolving with the primary goal to address the shift from traditional hub-and-spoke WAN architectures (from branch office to on-premises data center) to connect with more intelligent and distributed cloud services that are primarily internet-based resources. The specifications of some of the available hardware to implement smart SD-WAN edge connect is listed in Tab II. By adopting the latest advancements in the network architecture, several low latency and secure end-user applications can be implemented via SD-WAN and intelligent NGFW, mainly:

- A regional WAN that is typically a midsize OT with a smaller number of WAN locations (fewer than 50 sites or IoT sensing devices).
- A metropolitan WAN that has 200 or 1,000 sites, and that spans at least in a big city with increasing resources moving to the cloud.
- A large-scale retail WAN typified by small footprint locations (such as remote grid stations, solar energy sites, on-shore and off-shore windmills) that scales from hundreds to thousands of near-identical locations, either domestically or across multiple regions.
- A security-sensitive WAN is a mid- to large-scale deployment from 25 sites and higher that are focused on

TABLE II
SPECIFICATIONS OF UNITY-EDGE CONNECT SD-WAN HARDWARE PLATFORMS (SOURCE: SILVER PEAK)

	Edge Connect US	Edge Connect XS	Edge Connect S	Edge Connect M	Edge Connect L	Edge Connect XL
Architecture	Home Office	Small Branch	Large Branch	Small Hub	Large Hub	Data Center
Bandwidth	1-100 Mbps	2-200 Mbps	10-1000 Mbps	50-2000 Mbps	1-5 Gbps	2-10 Gbps
Connections	256,000	256,000	256,000	2,000,000	2,000,000	2,000,000
Average Throughput	25 Mbps	50 Mbps	200 Mbps	500 Mbps	1 Gbps	5 Gbps
Redundancy	No	No	No	Power and SSD	Power and SSD	Power and SSD
Interfaces	3xRJ45 10/100/1000	4xRJ45 10/100/1000	6xRJ45, Dual 1/10 Gbps short reach, or long reach fiber module (optional)	4xRJ45, 2x 1/10 Gbps fiber, fail-to-glass (bypass) 4xRJ45, 2xSFP plus (pluggable)	4xRJ45, 2x1/10 Gbps fiber, fial-to-glass (bypass) 4xRJ45, 2xSFP plus (Pluggable)	4x 1/10 Gbps fiber, fail-to-glass (bypass) 6x 1/10 Gbps SFP plus, 10/25 Gbps SFP28 (pluggable)

securing the data from the IoT edge devices to the cloud. These network architectures usually have multiple NGFW to secure the sensitive energy installations.

VII. CONCLUSIONS

SD-WAN is a software-based approach to wide area networks, essentially a virtual WAN for mission critical IoT and 5G applications. It can be used to connect any application with bandwidth and latency requirements using flexible communication frameworks, whether MPLS, 5G, 4G/LTE, or broadband Internet. SD-WAN offers QoS controls to differentiate data in multiple ways, and it offers business-driven solutions for challenges such as latency, high data rates, bandwidth, configuration, and performance. It also offers data-driven decision making capabilities and NGFW that can defend the network from external cyber attacks. While SD-WAN will build on the past successes of more mature technologies like SDN and WAN, it may hold the key to the promising future of our vast and growing global energy network ecosystem.

REFERENCES

[1] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113 – 1122, 2011.

[2] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[3] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[4] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1 – 11, 2011.

[6] Z. Duliński, G. Rzym, and P. Chołda, "Mpls-based reduction of flow table entries in sdn switches supporting multipath transmission," *Computer Communications*, vol. 151, pp. 365 – 385, 2020.

[7] M. L. Lakshmi and N. Bandaru, "Configuring mpls cloud providers with virtual private network," in *Innovations in Electrical and Electronics Engineering*, H. S. Saini, T. Srinivas, D. M. Vinod Kumar, and K. S. Chandragupta Mauryan, Eds. Singapore: Springer Singapore, 2020, pp. 817–826.

[8] Z. Duliński, R. Stankiewicz, G. Rzym, and P. Wydrych, "Dynamic traffic management for sd-wan inter-cloud communication," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1335–1351, 2020.

[9] I. Ellawindy and S. S. Heydari, "Qoe-aware real-time multimedia streaming in sd-wans," in *2019 IEEE Conference on Network Softwarization (NetSoft)*, 2019, pp. 66–71.

[10] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From iot to 5g i-iot: The next generation iot-based intelligent algorithms and 5g technologies," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 114–120, 2018.

[11] I. Ayadi, N. Simoni, and G. Diaz, "Naas: Qos-aware cloud networking services," in *2013 IEEE 12th International Symposium on Network Computing and Applications*, 2013, pp. 97–100.

[12] S. Erdheim, "Deployment and management with next-generation firewalls," *Network Security*, vol. 2013, no. 10, pp. 8 – 12, 2013.

[13] K. Alwasel *et al.*, "Iotsim-sdwan: A simulation framework for interconnecting distributed datacenters over software-defined wide area network (sd-wan)," *Journal of Parallel and Distributed Computing*, vol. 143, pp. 17 – 35, 2020.

[14] G. Gangadharan, "Open source solutions for cloud computing," *Computer*, vol. 50, no. 01, pp. 66–70, jan 2017.

[15] C. N. Sminesh, E. G. M. Kanaga, and A. Roy, "Optimal multi-controller placement strategy in sd-wan using modified density peak clustering," *IET Communications*, vol. 13, no. 20, pp. 3509–3518, 2019.

[16] K. Basu, A. Hamdullah, and F. Ball, "Architecture of a cloud-based fault-tolerant control platform for improving the qos of social multimedia applications on sd-wan," in *2020 13th International Conference on Communications (COMM)*, 2020, pp. 495–500.

[17] B. Soewito and C. E. Andhika, "Next generation firewall for improving security in company and iot network," in *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 2019, pp. 205–209.

[18] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2476–2486, 2020.

[19] Sandhya, Y. Sinha, and K. Haribabu, "A survey: Hybrid sdn," *Journal of Network and Computer Applications*, vol. 100, pp. 35 – 55, 2017.

[20] Y. Guo, Z. Wang, X. Yin, X. Shi, and J. Wu, "Traffic engineering in sdn/ospf hybrid network," in *2014 IEEE 22nd International Conference on Network Protocols*, 2014, pp. 563–568.

[21] M. Yang, H. Rastegarfar, and I. B. Djordjevic, "Secure bidirectional adaptive resource allocation in sdn-enabled 5g fronthaul networks," in *2018 Asia Communications and Photonics Conference (ACP)*, 2018, pp. 1–3.

[22] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, "An approach for the secure management of hybrid cloud–edge environments," *Future Generation Computer Systems*, vol. 90, pp. 1 – 19, 2019.